iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 7 **Issue:** XI **Month of publication:** November 2019

DOI: http://doi.org/10.22214/ijraset.2019.11037

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 7 Issue XI, Nov 2019- Available at www.ijraset.com

A Review of different Methods of Watermarking for Medical Images Authentication

Dhara Desai[1], Nisha Gandhi[2], Shruti Dodani[3]
[1,2,] *B.E Biomedical Engineering Department, Dwarkadas J Sanghvi College of Engineering, Mumbai.*
[3] *Assistant Professor, Dwarkadas J Sanghvi College of Engineering, Mumbai.*

Abstract: With advancement in communication technology, sharing of medical images over the internet is on rise. But with that it is always required to maintain the integrity of the images. Hence it is necessary to develop techniques for authentication. One solution to protect the digital medical images is by Digital image watermarking. This paper reviews different watermarking techniques for authentication of medical images.
Keywords: Watermarking, authentication, medical images, embedding, extraction, patient

I. INTRODUCTION

Results from instruments used in radiology such as CT, MRI, X-ray, Ultrasound etc. are stored in the form of images. These medical images need to be stored or transferred for diagnosis. However, these images can be easily distorted or modified, which will harm the patient's diagnosis. Therefore, it is necessary to maintain the integrity, security, and authenticity of these medical images. The authenticity of these images can be taken care of by performing technique called watermarking. Watermarking is a technique in which data that needs to be hidden is inserted using a carrier image/signal. The image on which the data is embedded is called a watermarked image. Embedding an image can be done using different techniques. Also after embedding an image, the original image has to be recovered properly for a reliable diagnosis to take place. This paper analyses different methods of embedding and extraction for image authentication and recovery.

II. LITERATURE REVIEW

A. Secure Hybrid Robust Watermarking Technique

This method is based on DWT-DCT and it improves the robustness and security of the watermarks without noteworthy devaluing of cover image quality against the attacks of signal processing [1]. The algorithmic steps are discussed below [1]:

1) Embedding Process

a) The cover image is divided into ROI and NROI parts, on which second-level DWT is applied to obtain the sub-bands as LL2, LH2, HL2 and HH2[1].

b) On the watermarked image, third-level DWT is applied and DCT transformation is applied to LL3 sub-band of the DWT watermark image [1]. The DCT transform of watermark image is formatted using modulus function to obtain watermark 'W1'.

c) The electronic patient record (EPR) data file is selected as text watermark and to obtain the watermark 'W2' the watermark is encrypted using public key cryptography.

d) To insert the image watermark into the ROI part of the cover image, Inverse discrete cosine transform (IDCT) and second-level inverse discrete wavelets transform (IDWT) is applied. And to insert data watermark in the NROI region, the second-level inverse discrete wavelet transform is applied.

e) The final watermarked image is formed by merging the embedded ROI and NROI parts of the medical cover image [1].

2) Extraction Process

a) The watermarked image is divided into the ROI and NROI parts.

b) On the NROI and ROI parts of the medical image cover, the 2nd-level DWT and 3rd-level DWT are applied respectively. And to the LL3 sub-band of ROI part of the cover, DCT transform is applied.

c) From the ROI and NROI part of the cover image [1], the watermark 'W1' and encrypted text watermark 'W2' are extracted respectively.

d) To obtain EPR data, the watermark 'W2' is decrypted using the public key cryptography.

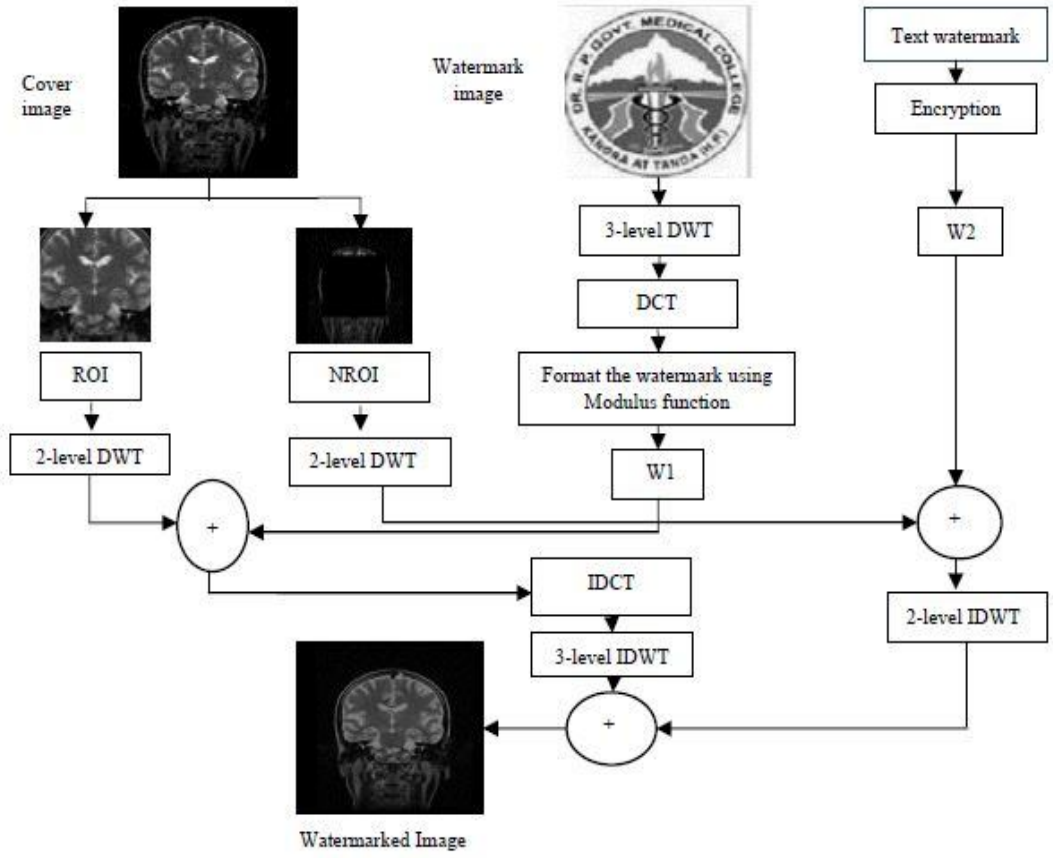


Fig. 1 Block diagram of embedding process [1]

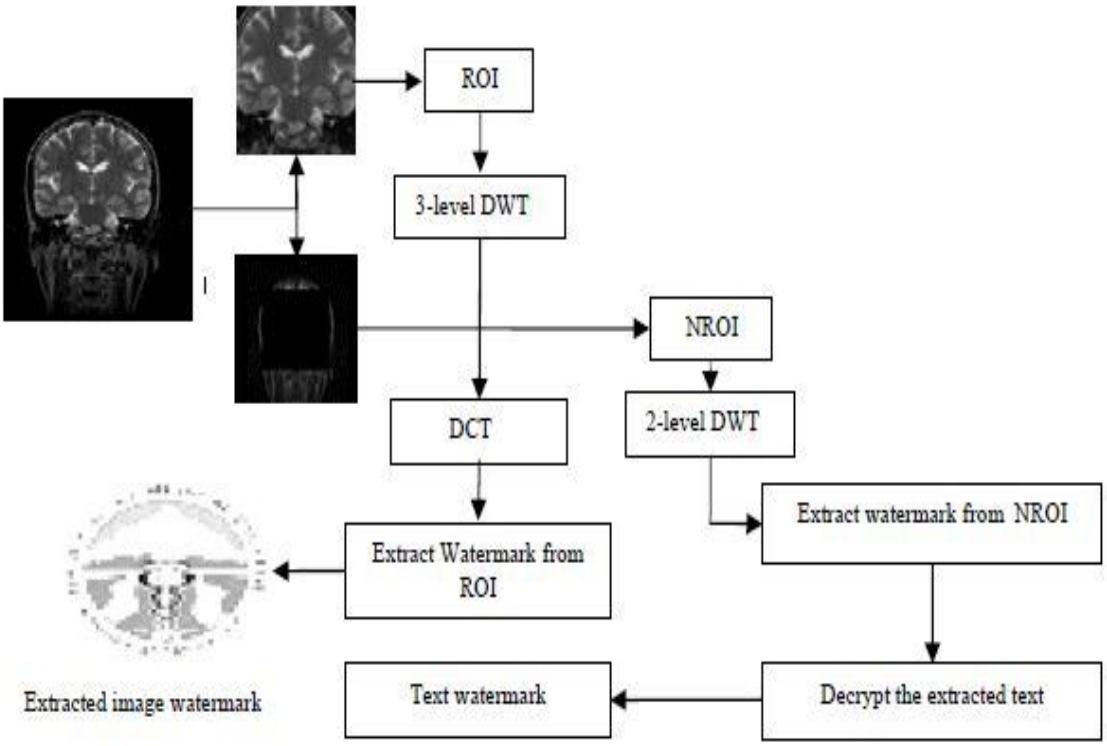


Fig. 2 Block diagram of extraction process [1]

B. DWT, SVD and Zero Watermarking

A zero-bit watermarking algorithm implementing one value decomposition and DWT was put forth by Wen-ge, Feng, and Liu Lei[2,5] The method was performed for medical images by [2]. The algorithm of the proposed method is as follows [2]:

1) Embedding Process

a) DWT is applied on the host image, which is used as input image. It divides the host image into four blocks LL, LH, HH, HL.

b) As LL sub band possesses maximum robustness, blocking is performed on it.

c) For unique feature extraction SVD is applied over the blocks.

d) Using XOR gate between the singular feature extraction and the watermark image, a master share image is obtained.

e) For security, scrambling algorithm [2] is performed on master share image.

f) Finally, the receiver receives the final master share image.

2) Extraction Process

a) For recovery, descrambling algorithm is performed.

b) 2-level DWT and then SVD [2] on the LL band is performed over the image sent along the final master share.

c) From (3) the singular feature is extracted.

d) Using the XOR gate between the singular feature extracted from the image and the master share image, the watermark image is obtained.

e) Successful the watermark is obtained. And it can be verified if any modifications were done to the image.

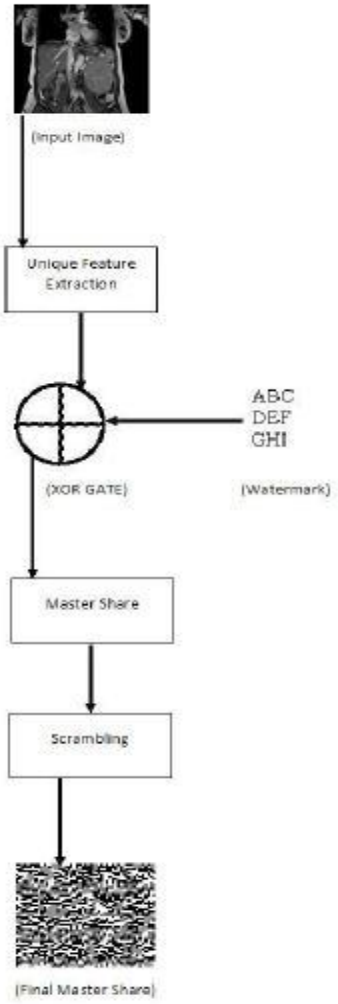


Fig. 3 Block diagram of proposed algorithm.[2]

C. A Lossless Watermarking Based Authentication.

In medical imaging, modification of least bit can lead to erroneous diagnosis [6,7,8], which were not acceptable as they were irreversible. Hence to provide reversible watermarking without causing any effect to the image. This method was proposed. The algorithm of this method is as follows [3]:

1) *Embedding Process:* When the image is scanned row wise the bit-stream of LSB are losslessly compressed. The compression is concatenated with the hash and patient details and embedded into LSBs by scanning the image. The procedure is explained in four steps:

a) Using MD5 algorithm, the authentication code (MAC) of the image is calculated.

b) MAC code and the patient details are concatenated and the resulting string is encrypted.

c) LSBs from all pixels is selected and the string obtained is compresses by RLE algorithm.

d) The compressed string and the encrypted string are concatenated and inserted back into the LSB location by adding any blanks if necessary [3].

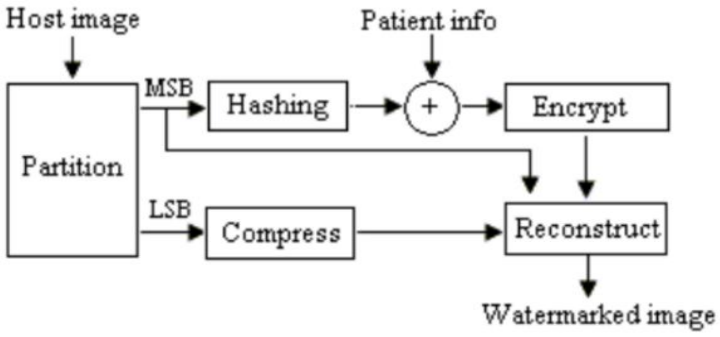


Fig. 4 Block Diagram of Embedding phase [3]

2) *Extraction Process*

a) Initially the image is scanned in the same way as in embedding process.

b) Actual MAC is calculated from MSBs and the concatenated bit-stream from LSBs is extracted, which is divided into two sections [3]:

i) The encrypted patient information and the MAC [3].

ii) The compressed LSBs of original image [3].

c) Using RLE decompressing algorithm the original bit-stream is obtained. By scanning we can recover the original bits to their original place in the image's LSBs.

d) Decryption of the extracted bit-stream gives the patient details and the original MAC.

e) Authentication and rejection of image is done by comparing the original MAC with the actual MAC.

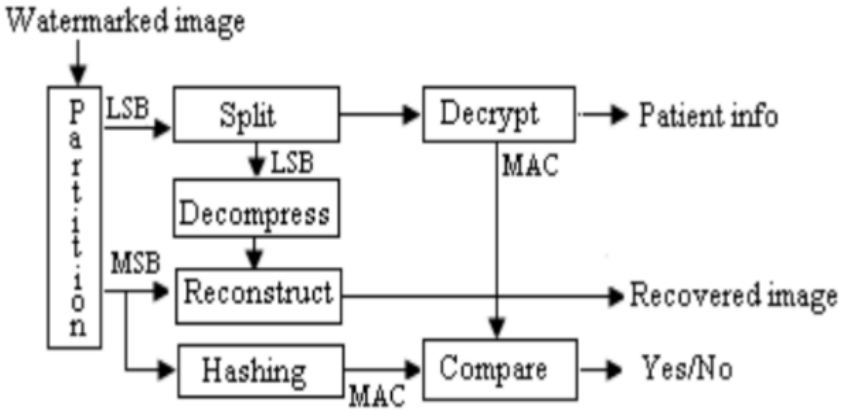


Fig. 5 Block diagram of Extraction and Authentication phase.[3]

III.INFERENCE

The table below shows advantages and disadvantages of the above methods for medical image authentication by watermarking. Each method has their own embedding and extraction process and it is difficult to determine which among them works best.

TABLE I

ADVANTAGES AND DISADVANTAGES OF THE METHODS

Method	Advantages	Disadvantages
Secure Hybrid Robust Watermarking Technique	It is robust against various signal processing attacks. It develops a high quality of watermarked image.	Any modifications on the image cannot be detected. The image can be tampered.
DWT, SVD and Zero Watermarking	It is a stable method. It provides unique identification of images. It is capable of tamper detection and authenticates the image.	~
A Lossless Watermarking based authentication	The image can be restored as the original image for a diagnosis. The size of the image remains same and no additional file has to be sent.	Tamper detection is not possible. It restricts the automation and easy use of authentication systems.

IV.CONCLUSIONS

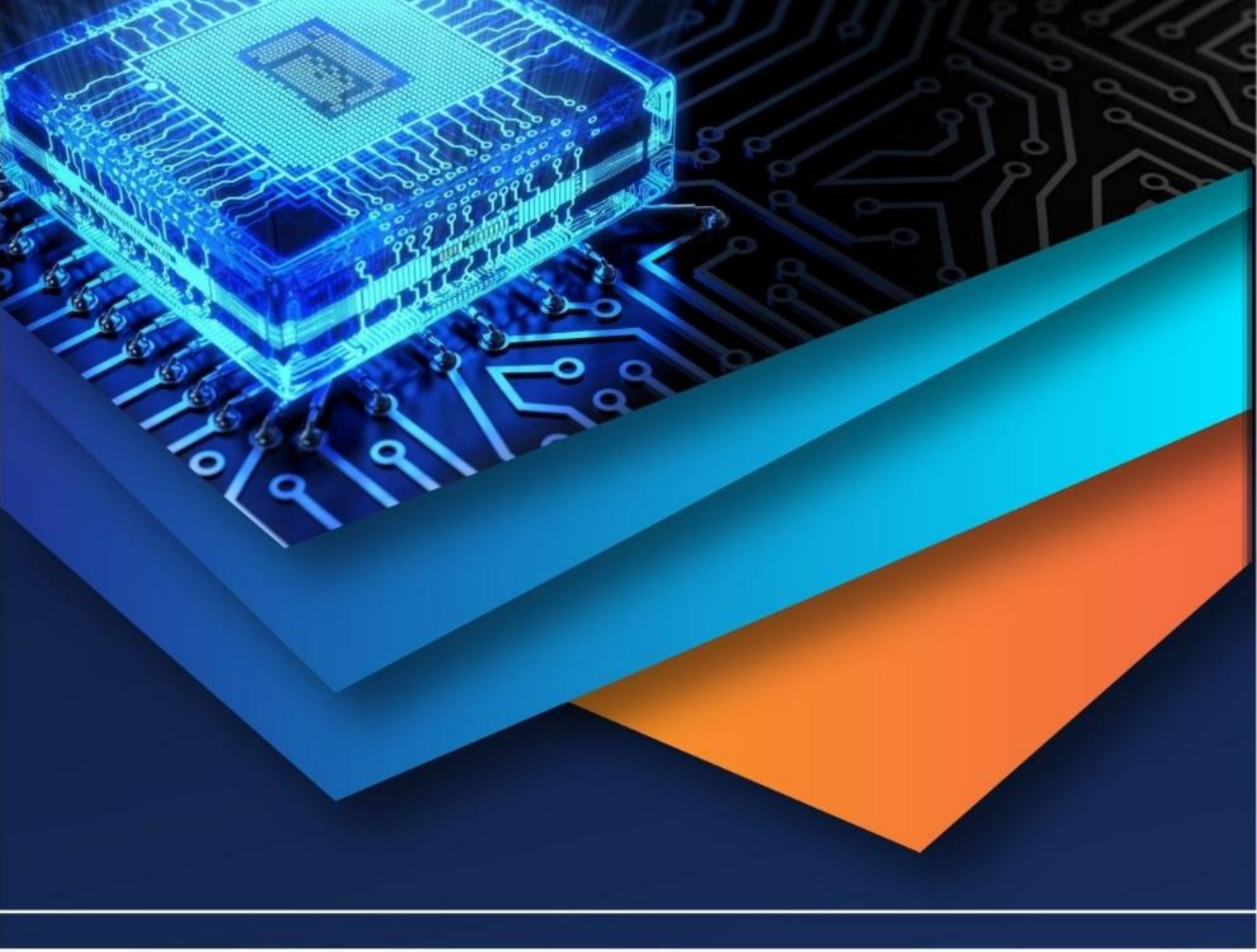
To conclude this research, the advantages and disadvantages about each method discussed above are tabulated. Different datasets have been used to test each of the method. The Secure Hybrid Robust Watermarking Technique is based on DWT and DCT and the private and restricted patient information is enhanced using public key cryptographic (RSA) techniques. The Zero Watermarking Technique is based on DWT and SVD methods. Also, PSNR (Peak signal to noise ratio) [4] is used to determine the quality of output image which further indicates the peak error. And in the Lossless Watermarking technique, HMAC, a keyed-hash authentication code [3] is used for authentication. No absolute values are used to represent the accuracy of the systems as there is no standardized testing benchmarks for testing purposes.

V. FUTURE WORKS

For a straight forward comparison between these methods, the techniques will be applied on a common dataset. Comparing these techniques will help establish common benchmarks.
Other researchers can benefit if some other robust techniques are also reviewed.

REFERENCES

[1] Abhilasha Sharma, Amit Kumar Singh* and S P Ghrera “Secure Hybrid Robust Watermarking Technique for Medical Images” 4th International Conference on Eco-friendly Computing and Communication Systems, ICECCS 2015
[2] Samman Sinha, Abhilasha Singh, Ritu Gupta, Shreyya Singh “Authentication and Tamper Detection in Tele-medicine using Zero Watermarking” International Conference on Computational Intelligence and Data Science (ICCIDS 2018)
[3] Samia Boucherkha and Mohamed Benmohamed “A Lossless Watermarking Based Authentication System For Medical Images” International Journal of Medical, Health, Biomedical, Bioengineering and Pharmaceutical Engineering Vol:1, No:1, 2007
[4] Abhilasha Singh and Malay Kishore Dutta “Wavelet-based reversible watermarking system for integrity control and authentication in tele-ophthalmological applications”, Int. J. Electronic Security and Digital Forensics, Vol. 8, No. 4, 2016
[5] Wen-ge, Feng, and Liu Lei. "SVD and DWT zero-bit watermarking algorithm." Informatics in Control, Automation and Robotics (CAR), 2010 2nd International Asia Conference on. Vol. 3. IEEE, 2010.
[6] F. Hartung and M. Kutter, “Multimedia watermarking techniques,” Proceedings of the IEEE, vol. 87, no. 7,pp. 1079–1107, July 1999.
[7] A. J. Menezes, P. C. Van Oorschot, S. A. Vanstone, "Handbook of Applied Cryptography", CRC Press, 1997.
[8] J. Fridrich, M. Goljan and R. Du, “Invertible Authentication, Proc. SPIE Photonics West, vol. 3971, Security and Watermarking of Multimedia “ Contents III, pp. 197-208, 2001.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY